Consumer IoT Security Quick Guide:

NO UNIVERSAL DEFAULT PASSWORDS

IoT Security Foundation

No Universal Default Passwords

New standards and regulation

A newly connected IoT device is attacked within five minutes.[1] To improve security, new standards and upcoming regulations require IoT manufacturers, and some importers, using passwords in their IoT products to ensure provided passwords are unique per device. As a result, companies need to assess how their IoT products use passwords.

Standard ETSI EN 303 645[2] requires that products do not use "universal default passwords". The UK Government's Code of Practice for Consumer IoT Security[3], US California Senate Bill #327[4] and Oregon House Bill #2395[5], and Australian Draft Code of Practice[6] set out similar requirements. The UK government is preparing legislation which will prohibit the use of universal default passwords in consumer IoT.[7]

Important security considerations

"No universal default passwords" is an important provision because default passwords that are easily guessable or derivable weaken security. If a *universal* default password is used (i.e. one password used across multiple devices) once one device is compromised, all devices using the same default password can be compromised. Poor password practices have the potential to put users' and businesses' personal data, devices and networks at risk. Moreover, business users of consumer IoT run the risk of financial or reputational damage. By contrast, good password practices help prevent unauthorised access. In some cases the elimination of passwords through the use of alternative non-password based authentication and authorisation mechanism may be more appropriate and easier to use. Not relying on passwords lessens the burden on users.

Impact on consumer IoT manufacturers

Failure to comply with existing standards or regulation can result in significant reputational and financial damage to an IoT manufacturer or importer. For instance, California Bill #327 currently sets no bounds for financial penalties nor does it scope potential obligations (e.g. increased oversight or audits). Forthcoming UK regulation will likely result in sanctions, such as fines or the removal of non-compliant products from the market.

Why it matters

- Users are unlikely to change a password unless forced to – increasing risks associated with universal passwords.
- Universal passwords can be a vulnerability for IoT devices and their users.
- Poorly managed/used passwords put users, personal data, and devices at risk.
- Attackers can co-opt devices with weak passwords, putting networks and connected things at risk.
- Failure to comply with existing standards or regulation can result in reputational and financial damage.

Where to start?

Below are five key questions for managers to discuss among product development, security, and compliance teams which will help on the road to compliance with ESTI EN 303 645.[2]

- Is using a password the best solution for our product or could a stronger proven authentication mechanism be used?
- Do we use universal default passwords?
- Do we use default passwords? If we do, are they unique-per-device and not easy to guess or derivable?
- Are passwords a vulnerability in our design?
- Do we follow industry best practices for passwords (e.g. UK NCSC[8] and NIST[9])?

Existing standards, regulation and guidance

- ETSI EN 303 645 Cyber Security for Consumer IoT (2020)[2]
- UK DCMS Code of Practice for Consumer IoT Security (2018)
- United States: California and Oregon state legislation
- Australia Draft Code of Practice: Securing the Internet of Things
- Upcoming UK Regulation for Consumer IoT Security (2021)

Dos and Don'ts: Guidance on complying with new standards and regulation

Dos

Guidelines apply to all product passwords (including web/API interfaces) not only user-facing passwords

Assess if passwords are necessary for your product.

- Understand how and why your product is using passwords, and determine if it is necessary or is the best solution for the product.
- Understand what part(s) of the product or service needs controlled access.
- Identify if using alternative authentication and authorisation mechanisms will improve usability and security.
- Consider other non-password or technical solutions - for example, NFC, Bluetooth, biometrics or temporal proximity methods. Also consider innovations or new specifications[10] and methods such as OAuth for smart phones and apps.

If passwords are right for your product, follow these guidelines:

Default passwords

- Default passwords (like those pre-installed and printed on instructions) must be unique, must not be easily guessable, or be related to public information (e.g. MAC address or Wi-Fi SSID) in an obvious way.
- When using pre-installed unique-per-device passwords, generate these with a random mechanism that reduces the risk of automated attacks.

User password management

- Provide a secure initial password and do not force users to change it during product setup. Have the user change and/or setup passwords before the device can be used if a universal default password, poor password, or no password is provided.
- Make sure passwords are recoverable or resettable, for example in the event of loss of a unique or secure password so that users can continue to use/access the product and its features. This may include resetting to an original unique password.
- Users must be able to (re)set passwords if needed.
- Have a user-friendly[12] and practical password policy that follows up-to-date best practices to guide users when setting passwords.

Don'ts

- Do not use **any** universal passwords (e.g. "admin/admin"). Passwords must be unique to each product/device.
- Do not use a default password unless necessary.
- If using default passwords are necessary, they must not be derivable, for instance by using a published formula or serial number.
- Passwords must not be easily guessable, such as a MAC address or a commonly used password like "12345".
- A list of commonly used (and hacked) passwords is regularly updated and available at HaveIBeenPwned.com.[13]

Keep passwords secure

- Protect communication and storage of passwords, for instance on the device and in transit.
- Industry standard methods should be used to protect passwords when storing them or transferring them across networks. For more information, see the IoTSF Best Practice Guide Release 2, section F on "credential management".[11]

Adopt best practices

- UK National Cyber Security Centre – Password Guidance: Simplifying Your Approach (2016).[8]
- USA National Institute of Standards and Technology (NIST) Special Publication 800-63B – Digital Identity Guidelines - Authentication and Lifecycle Management (2017).[9]
- IoT Security Foundation Best Practice Guides – Credential Management (2019).[11]

Things to think about going forward

In addition to the basic dos and don'ts, here are a few more areas that need to be considered when using passwords in consumer IoT products.

- Make set-up and continuing password management easy for users.
- Build in brute-force attack protection. For examplr, limit the rate at which passwords can be tried.
- Consider if phasing out passwords is a viable option for the product – and for those products already on the market and in use. Could secure non-password authentication be an option for future releases?

Where to go for more information?

From the IoT Security Foundation

- IoTSF Best Practice Guides[11]
- IoTSF consumer IoT security webpage[14]
- IoTSF's live training webinars

From other bodies

- Japan's IoT Security Guidelines v1.0[15]
- Mozilla's Don't Get Pwned: A Guide to Safer Logins[16]

Who should see this:

It is critical that people with different roles and responsibilities are aware of default password standards and regulations, and how they impact the organization and products. Examples of who should see this include:

Compliance officer: The compliance officer is responsible for how the organization respects the principles in this guide, standards, regulations and codes of practice.

Product Manager: Buy in from the product manager is also critical. The product manager needs to see how the product fits into existing ecosystems of IoT products (such as smart speaker systems), and to plan how the product may integrate into them. Key to all of those ecosystems is the authorization scheme.

Head of Design: Designers will have to implement one or more designs for initial onboarding, and this effort should not be left to the end (security last), but if done early, then the security by design process will become a critical path. The UX evaluation does not have to occur on the real product, particularly if it uses a web interface.

User Experience (UX) Manager: The initial onboarding and user authorization flow is the first experience every user will have. Getting this correct is critical, and this aspect of design cannot be done later. A cross section of potential users should be considered and involved in early design phases.

Head of Marketing and PR: The UX usually reports to marketing. The security flow needs to be among the top concerns. Getting it wrong, or leaving it too late, will reflect badly on the product and the company that produced it.

What are the Consumer IoT Security Quick Guides?

The "Consumer IoT Security Quick Guides" identify best practices to help organisations around the world understand and comply with new international standards, regulations and national guidance on consumer IoT security. These Quick Guides demystify high level language, point to additional information, and provide different ways of thinking about or alternative approaches to consumer IoT security.

The Quick Guides build upon the ETSI EN 303 645[2] specification on consumer IoT cybersecurity. It is the first international standard of its kind. Based upon it, governments are publishing guidance[17] and are preparing legislation[18] that impact companies developing, manufacturing or providing consumer IoT products. The Quick Guide series focuses on the top 3 issues identified in standards and guidance: passwords, vulnerability disclosure, and software updates.[3]

Footnotes

1. https://www.netscout.com/sites/default/files/2019-02/SECR_001_EN-1901%20-%20NETSCOUT%20Threat%20Intelligence%20Report%202H%202018.pdf
2. https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf
3. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/773867/Code_of_Practice_for_Consumer_IoT_Security_October_2018.pdf
4. https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB327
5. https://olis.leg.state.or.us/liz/2019R1/Measures/Overview/HB2395
6. https://www.homeaffairs.gov.au/reports-and-pubs/files/code-of-practice.pdf
7. The regulatory proposals are currently subject to a public call for views and might change as a result.
8. See https://www.ncsc.gov.uk/collection/passwords
9. https://pages.nist.gov/800-63-3/sp800-63b.html
10. For example, those being developed by industry associations such as the FIDO Alliance, https://fidoalliance.org/overview/
11. https://www.iotsecurityfoundation.org/wp-content/uploads/2019/12/Best-Practice-Guides-Release-2_Digitalv3.pdf
12. For example, letting people paste passwords https://www.ncsc.gov.uk/blog-post/let-them-paste-passwords
13. https://haveibeenpwned.com/
14. http://www.iotsecurityfoundation.org/consumer-iot
15. http://www.iotac.jp/wp-content/uploads/2016/01/IoT-Security-Guidelines_ver.1.0.pdf
16. https://blog.mozilla.org/internetcitizen/2017/01/25/better-password-security/
17. For example, the UK and Australia
18. For example, US states Oregon and California, and the UK.

Acknowledgements

This guidance was commissioned by the Department for Digital, Culture, Media & Sport (DCMS) and delivered by the IoT Security foundation in partnership with Oxford Information Labs.

We wish to acknowledge significant contributions from IoTSF members to this version of the document

Stacie Hoffmann and Patrick Taylor, Oxford Information Labs
Michael Richardson, Sandelman Software Works

Peer reviewers:
Roger Shepherd, Chipless
Trevor Hall, DisplayLink
Richard Marshall, Xitex Ltd
Claire Milne, independent consultant

Plus others – you know who you are!

IoT Security Foundation

Department for Digital, Culture, Media & Sport

In partnership with OXFORD INFORMATION LABS